(12) NACH DEM VERTRAG ÜBER DIE INTERNATIONALE ZUSAMMENARBEIT AUF DEM GEBIET DES PATENTWESENS (PCT) VERÖFFENTLICHTE INTERNATIONALE ANMELDUNG

(19) Weltorganisation für geistiges Eigentum
Internationales Büro

(43) Internationales Veröffentlichungsdatum
25. September 2003 (25.09.2003)

PCT

(10) Internationale Veröffentlichungsnummer
WO 03/079609 A1

(51) Internationale Patentklassifikation[7]: H04L 9/32, G07B 17/00

(21) Internationales Aktenzeichen: PCT/DE03/00760

(22) Internationales Anmeldedatum:
10. März 2003 (10.03.2003)

(25) Einreichungssprache: Deutsch

(26) Veröffentlichungssprache: Deutsch

(30) Angaben zur Priorität:
102 11 265.7 13. März 2002 (13.03.2002) DE

(71) Anmelder *(für alle Bestimmungsstaaten mit Ausnahme von US)*: **DEUTSCHE POST AG** [DE/DE]; Charles-de-Gaulle-Str. 20, 53113 Bonn (DE).

(72) Erfinder; und

(75) Erfinder/Anmelder *(nur für US)*: **MEYER, Bernd** [DE/DE]; Zum Stöckerhof 2 c, 53639 Königswinter (DE). **LANG, Jürgen** [DE/DE]; Schau ins Land 15, 51429 Bergisch Gladbach (DE).

(74) Anwalt: **PATENTANWÄLTE JOSTARNDT - THUL**; Brüsseler Ring 51, 52074 Aachen (DE).

(81) Bestimmungsstaaten *(national)*: AE, AG, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BY, BZ, CA, CH, CN, CO, CR, CU, CZ, DK, DM, DZ, EC, EE, ES, FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MA, MD, MG, MK, MN, MW, MX, MZ, NI, NO, NZ, OM, PH, PL, PT, RO, RU, SC, SD, SE, SG, SK, SL, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, YU, ZA, ZM, ZW.

(84) Bestimmungsstaaten *(regional)*: ARIPO-Patent (GH, GM, KE, LS, MW, MZ, SD, SL, SZ, TZ, UG, ZM, ZW), eurasisches Patent (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), europäisches Patent (AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HU, IE, IT, LU, MC, NL, PT, RO, SE, SI, SK, TR), OAPI-Patent (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, ML, MR, NE, SN, TD, TG).

Erklärungen gemäß Regel 4.17:

— *hinsichtlich der Berechtigung des Anmelders, ein Patent zu beantragen und zu erhalten (Regel 4.17 Ziffer ii) für die folgenden Bestimmungsstaaten AE, AG, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BY, BZ, CA, CH, CN, CO, CR, CU, CZ, DK, DM, DZ, EC, EE, ES, FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MA, MD, MG, MK, MN, MW, MX, MZ, NI, NO, NZ, OM, PH, PL, PT, RO, RU, SC, SD, SE, SG, SK, SL, TJ, TM, TN, TR, TT, TZ, UA, UG, UZ, VC, VN, YU, ZA, ZM, ZW, ARIPO-Patent (GH, GM, KE, LS, MW, MZ, SD, SL, SZ, TZ, UG, ZM, ZW), eurasisches Patent (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), europäisches Patent (AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HU,*

[Fortsetzung auf der nächsten Seite]

(54) Title: METHOD AND DEVICE FOR THE GENERATION OF CHECKABLE FORGERY-PROOF DOCUMENTS

(54) Bezeichnung: VERFAHREN UND VORRICHTUNG ZUR ERSTELLUNG PRÜFBAR FÄLSCHUNGSSICHERER DOKUMENTE

(57) Abstract: The invention relates to a method and a device for the generation of checkable forgery-proof documents with an externally supplied cryptographic module, whereby the checking of authenticity of the document is carried out without using key information belonging to the cryptographic module. According to the invention, the method and the device are characterised in that the cryptographic module is supplied with two types of data, even on supply from a communication partner which is cryptographically not trustworthy, which either remain in the cryptographic module or are attached to the document. The information remaining in the cryptographic module is used to secure the document information by means of a check value and the information transferred into the document serves to verify the securing of the document by the cryptographic module during a check of the authenticity of the document at a checkpoint.

(57) Zusammenfassung: Die Erfindung betrifft ein Verfahren und eine Vorrichtung zur Erstellung prüfbar fälschungssicherer elektronischer Dokumente mit einem extern gespeisten kryptografischen Modul, wobei die Prüfung der Unverfälschtheit der Dokumente ohne Benutzung von Schlüsselinformationen erfolgt, die dem kryptografischen Modul eigen sind. Erfindungsgemäß zeichnen sich das Verfahren und die Vorrichtung dadurch aus, dass das kryptografische Modul auch bei einer Speisung über kryptografisch nicht vertrauenswürdige Kommunikationspartner mit zwei Arten von Daten versorgt wird, die zum einen im kryptografischen Modul verbleiben und die zum anderen an das Dokument angehängt werden, wobei die im kryptografischen Modul verbleibenden Informationen genutzt werden, um die Dokumentinformationen über einen Prüfwert abzusichern und wobei die in das Dokument übernommenen Informationen dazu dienen, im Rahmen einer Prüfung der Unverfälschtheit des Dokuments in einer Prüfstelle die Absicherung des Dokuments durch das kryptografische Modul nachzuweisen.

WO 03/079609 A1

IE, IT, LU, MC, NL, PT, RO, SE, SI, SK, TR), OAPI-Patent (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, ML, MR, NE, SN, TD, TG)

— *Erfindererklärung (Regel 4.17 Ziffer iv) nur für US*

Veröffentlicht:

— *mit internationalem Recherchenbericht*

— *vor Ablauf der für Änderungen der Ansprüche geltenden Frist; Veröffentlichung wird wiederholt, falls Änderungen eintreffen*

Zur Erklärung der Zweibuchstaben-Codes und der anderen Abkürzungen wird auf die Erklärungen ("Guidance Notes on Codes and Abbreviations") am Anfang jeder regulären Ausgabe der PCT-Gazette verwiesen.

Verfahren und Vorrichtung zur Erstellung prüfbar fälschungssicherer Dokumente

Beschreibung:

Die Erfindung betrifft ein Verfahren zur Erstellung fälschungssicherer Dokumente oder Datensätze, wobei eine Schlüsselinformation erzeugt und eine verschlüsselte Prüfinformation aus der Schlüsselinformation und einem Transaktions-Indikator gebildet wird.

Die Erfindung betrifft ferner ein Wertübertragungszentrum und ein kryptografisches Modul.

Es ist eine Vielzahl von Verfahren zur Erzeugung fälschungssicherer Dokumente und zu ihrer Überprüfung bekannt. Übliche Verfahren basieren auf der Erstellung digitaler Signaturen oder verschlüsselter Prüfinformationen, die im Rahmen der Erstellung des Dokuments angefertigt werden.

Zu unterscheiden ist dabei zwischen Dokumenten, bei denen der Ersteller ein Interesse an der Unverfälschtheit hat und solchen, bei denen Dritte ein Interesse an der Unverfälschtheit haben.

Hat ein Dritter Interesse an der Fälschungssicherheit von Dokumenten, so ist es bekannt, dass bei der Erstellung des Dokuments ein sogenanntes „kryptografisches Modul" hinzugezogen wird. Solche bekannten kryptografischen Module zeichnen sich dadurch aus, dass sie in ihrem Inneren elektronische Daten beinhalten oder Daten verarbeiten, die von außen nicht unbemerkt eingesehen oder manipuliert werden können.
Ein kryptografisches Modul kann als sichere, versiegelte Einheit betrachtet werden, in der sicherheitsrelevante Prozesse

durchgeführt werden, die von außen nicht manipuliert werden können. Ein weltweit anerkannter Standard für solche kryptografischen Module ist der von der US-amerikanischen nationalen Behörde für Standardisierung NIST veröffentlichte Standard für kryptografische Module mit der Bezeichnung FIPS Pub 140.

Wird zur Erstellung fälschungssicherer Dokumente, an deren Unverfälschtheit Dritte interessiert sind, ein kryptografisches Modul eingesetzt, so besteht eine übliche Realisierung darin, dass das kryptografische Modul genutzt wird, um kryptografische Schlüssel sicher zu hinterlegen, die innerhalb des Moduls, und nur dort, zur Verschlüsselung von Prüfwerten dienen. Bekannt sind beispielsweise sogenannte Signaturkarten, wie sie von Zertifizierungsbehörden oder Trustcentern zur Erstellung von digitalen Signaturen ausgegeben werden. Auch diese Signaturkarten, ausgeführt als Mikroprozessor-Chipkarte, enthalten in eben diesem Microporzessor-Chip ein kryptografisches Modul.

In solchen Modulen sind in der Regel ein oder mehrere asymmetrische Schlüsselpaare hinterlegt, die sich dadurch auszeichnen, dass Verschlüsselungen, die mit dem sogenannten privaten Schlüssel erzeugt werden, nur mit dem zugehörigen öffentlichen Schlüssel rückgängig gemacht werden können und dass Verschlüsselungen, die mit dem öffentlichen Schlüssel erzeugt werden, nur mit dem zugehörigen privaten Schlüssel rückgängig gemacht werden können. Gemäß ihrer Bezeichnung sind öffentliche Schlüssel dabei zur Veröffentlichung und beliebigen Verbreitung vorgesehen, wogegen private Schlüssel nicht ausgegeben werden dürfen und bei einer Verwendung zusammen mit kryptografischen Modulen diese Module zu keinem Zeitpunkt verlassen dürfen. Weiterhin hinterlegt in solchen Modulen sind Algorithmen etwa zur Prüfsummenbildung oder, im Beispiel der digitalen Signatur, zur Erstellung eines sogenannten digitalen Fingerabdrucks oder „Hash-Werts", der sich dadurch auszeichnet, dass er beliebigen Dateninhalt auf eine in der Regel quantitativ deutlich verkürzte Information der-

art abbildet, dass das Resultat irreversibel und eindeutig ist und dass für verschiedene Dateninhalte, mit denen der Algorithmus gespeist wird, jeweils unterschiedliche Resultate entstehen.

Die Erstellung eines fälschungssicheren Dokuments, an dessen Unverfälschtheit Dritte interessiert sind, mittels eines kryptografischen Moduls, das asymmetrische Schlüssel und einen Algorithmus zur Erstellung von Prüfwerten enthält, geschieht üblicherweise wie folgt: Zunächst wird unter Anwendung des Algorithmus zur Erstellung von Prüfwerten ein solcher Prüfwert erstellt, der sich auf das zu sichernde Dokument bezieht. Dann wird ein privater Schlüssel im kryptografischen Modul benutzt, um den Prüfwert zu verschlüsseln. Die Kombination dieser beiden Vorgänge wird als Erstellung einer „digitalen Signatur" bezeichnet.

Die Prüfung einer solchen digitalen Signatur geschieht üblicherweise wie folgt: Der Empfänger erhält das Dokument und den verschlüsselten Prüfwert. Der Empfänger benötigt weiterhin, und darauf zielt die später geschilderte Erfindung ab, den öffentlichen Schlüssel des Dokumentherstellers und verwendet diesen zur Entschlüsselung des Prüfwerts, den der Dokumentherstellers mit seinem privaten Schlüssel innerhalb des kryptografischen Moduls verschlüsselt hatte. Nach der Entschlüsselung besitzt der Empfänger somit den unverschlüsselten Prüfwert. Weiterhin wendet der Empfänger im nächsten Schritt den gleichen Algorithmus zur Erstellung eines Prüfwerts auf das empfangene Dokument an. Im dritten Schritt schließlich vergleicht der Empfänger den selbst erzeugten Prüfwert mit dem entschlüsselten Prüfwert des Dokumentherstellers. Stimmen beide Prüfwerte überein, so wurde das Dokument nicht verfälscht und die Unverfälschtheit des Dokuments ist zweifelsfrei nachgewiesen. Üblicherweise wird bei bekannten digitalen Signaturen auch die Authentizität des Dokument-

herstellers geprüft. Dies geschieht, indem der öffentliche Schlüssel des Dokumentherstellers von einer sogenannten Zertifizierungsstelle oder „CA" ebenfalls digital signiert und einem bestimmten kryptografischen Modul, beziehungsweise einem bestimmten Inhaber des kryptografischen Moduls, zugeordnet wird. Der Empfänger des Dokuments nimmt in diesem Fall den öffentlichen Schlüssel des Dokumentherstellers nicht einfach als gegeben an, sondern überprüft diesen ebenfalls auf Zugehörigkeit zum Dokumenthersteller, indem er die digitale Signatur des öffentlichen Schlüssels in der oben geschilderten Weise überprüft.

Bei diesen bekannten Verfahren besteht das Problem, dass zur Prüfung der Unverfälschtheit eines Dokuments eine Information erforderlich ist, die unmittelbar mit der Verwendung von Schlüsseln durch den Dokumenthersteller mittels des kryptografischen Moduls zusammenhängt. Im oben angeführten üblichen Beispiel der Erstellung von digitalen Signaturen handelt es sich um den öffentlichen Schlüssel des Dokumentherstellers bzw. dessen kryptografischen Moduls, der zur Prüfung herangezogen werden muss. Im Falle der Signatur des öffentlichen Schlüssels durch eine Zertifizierungsstelle wird das Gesamtgebilde aus öffentlichem Schlüssel, Identifikation des Anwenders dieses Schlüssels sowie der digitalen Signatur der Zertifizierungsstelle als „Schlüsselzertifikat" bezeichnet.

Zusammengefasst lässt sich diese Problematik an einem Beispiel derart schildern, dass es zur Prüfung der Unverfälschtheit eines üblichen digital signierten Dokuments erforderlich ist, den öffentlichen Schlüssel oder das Schlüsselzertifikat des Dokumentherstellers bzw. seines kryptografischen Moduls bei der Prüfung zur Verfügung zu haben. Sollen an einer Prüfstelle, wie üblich, Dokumente verschiedener Dokumentherstellers geprüft werden, so ist es erforderlich, dort alle öffentlichen Schlüssel oder alle Schlüsselzertifikate aller Doku-

menthersteller zur Verfügung zu haben.

Es existieren verschiedene Möglichkeiten, der Anforderung gerecht zu werden, den öffentlichen Schlüssel des Dokumentherstellers bei der Prüfung zur Verfügung zu haben. So ist es möglich, den öffentlichen Schlüssel oder das Schlüsselzertifikat des Dokumentherstellers an das zu sichernde Dokument anzuhängen. Eine weitere Möglichkeit besteht darin, den öffentlichen Schlüssel an der Prüfstelle zu hinterlegen und bei Bedarf auf diesen zuzugreifen.

Die bekannten Verfahren sind jedoch mit Nachteilen verbunden.

Das Anhängen des Schlüssels oder des Schlüsselzertifikats ist dann nachteilig, wenn der Umfang des Dokuments möglichst gering gehalten werden muss und ein angehängter Schlüssel den zu druckenden, zu übertragenden oder zu verarbeitenden Datensatz übermäßig vergrößern würde.

Eine Hinterlegung eines öffentlichen Schlüssels an der Prüfstelle ist insbesondere dann nachteilig, wenn ein Zugriff auf an der Prüfstelle hinterlegte Schlüssel aus praktischen oder zeitlichen Erwägungen nicht möglich ist, beispielsweise bei einer sehr hohen Anzahl von vorgehaltenen Schlüsseln, auf die in sehr kurzer Zeit zugegriffen werden müsste.

Zur Lösung dieser bekannten Nachteile ist es aus der Deutschen Patentschrift DE 100 20 563 C2 der Anmelderin bekannt, bei einem gattungsgemäßen Verfahren in einem Sicherungsmodul ein Geheimnis zu erzeugen, das Geheimnis zusammen mit Informationen, die Auskunft über die Identität des Sicherungsmoduls geben, verschlüsselt an eine Bescheinigungsstelle zu übergeben, das Geheimnis in der Bescheinigungsstelle zu entschlüsseln, hierdurch die Identität des Sicherungsmoduls zu erkennen, anschließend das Geheimnis zusammen mit Informa-

tionen zur Identität des Dokumentherstellers derart zu verschlüsseln, dass nur eine Prüfstelle eine Entschlüsselung vornehmen kann, um dann das Geheimnis an einen Dokumenthersteller zu übermitteln. Bei diesem Verfahren gibt der Dokumenthersteller eigene Daten in das Sicherungsmodul ein, wobei das Sicherungsmodul die selbst von dem Dokumenthersteller eingebrachten Daten mit dem Geheimnis irreversibel verknüpft und wobei keine Rückschlüsse auf das Geheimnis möglich sind. Dieses bekannte Verfahren zeichnet sich dadurch aus, dass das Ergebnis der irreversiblen Verknüpfung der von dem Dokumenthersteller eingebrachten Daten mit dem Geheimnis, die von dem Dokumenthersteller selbst eingebrachten Daten sowie die verschlüsselten Informationen der Bescheinigungsstelle das Dokument bilden, das an die Prüfungsstelle übermittelt wird. Dieses bekannte Verfahren eignet sich insbesondere zur Erzeugung und Prüfung fälschungssicherer Briefmarken eines Postunternehmens. Solche Briefmarken werden durch Kunden eines Postunternehmens unter Verwendung eines persönlichen kryptografischen Moduls erzeugt und als maschinenlesbarer Barcode auf die Sendung aufgebracht. Der maschinenlesbare Barcode hat nur einen sehr begrenzten Datenumfang und erlaubt es somit nicht, den öffentlichen Schlüssel des Kunden mit einzubringen. Außerdem müssen in der sogenannten Briefproduktion die digitalen Briefmarken in kürzester Zeit gelesen und geprüft werden, wodurch die Möglichkeit, in Sekundenbruchteilen auf eine Datenbasis von möglicherweise vielen Millionen öffentlicher Schlüssel zuzugreifen, ebenfalls entfällt.

Der Erfindung liegt die Aufgabe zugrunde, ein bekanntes Verfahren so weiter zu entwickeln, dass es unabhängig von einer unmittelbaren Kommunikation zwischen der kryptografisch vertrauenswürdigen Kontaktstelle und dem Dokumenthersteller durchgeführt werden kann.

Erfindungsgemäß wird diese Aufgabe dadurch gelöst, dass die Erstellung der zufälligen Schlüsselinformation und die Bildung der verschlüsselten Prüfinformation aus der Schlüsselinformation und dem Transaktionsindikator in einer kryptografisch vertrauenswürdigen Kontaktstelle erfolgen, dass die kryptografisch vertrauenswürdige Kontaktstelle die Schlüsselinformation verschlüsselt, und dass die verschlüsselte Prüfinformation und die verschlüsselte Schlüsselinformation von der kryptografisch vertrauenswürdigen Kontaktstelle an eine Zwischenstelle übermittelt werden, dass die Zwischenstelle die verschlüsselte Schlüsselinformation und die verschlüsselte Prüfinformation zwischenspeichert und zu einem späteren Zeitpunkt zeitlich von der Übertragung zwischen der kryptografisch vertrauenswürdigen Kontaktstelle und der Zwischenstelle entkoppelt an ein kryptografisches Modul eines Dokumentherstellers übermittelt.

Die Erfindung sieht somit vor, dass das kryptografische Modul auch bei einer Speisung über eine Zwischenstelle, beispielsweise über im kryptografischen Sinn nicht vertrauenswürdige Kommunikationspartner mit zwei Arten von Daten versorgt wird, die zum einen im kryptografischen Modul verbleiben und die zum anderen an das Dokument angehängt werden, wobei die im kryptografischen Modul verbleibenden Informationen genutzt werden, um die Dokumentinformationen über einen Prüfwert abzusichern und wobei die in das Dokument übernommenen Informationen dazu dienen, im Rahmen einer Prüfung der Unverfälschtheit des Dokuments in einer Prüfstelle die Absicherung des Dokuments durch das kryptografische Modul nachzuweisen.

Die Erfindung beinhaltet eine Vielzahl von Vorteilen. Sie ermöglicht eine Erzeugung fälschungssicherer Dokumente in einer Vielzahl von Anwendungsfällen, insbesondere bei solchen Fällen, bei denen keine direkte Verbindung zwischen dem Doku-

menthersteller und der vertrauenswürdigen Kontaktstelle besteht. Beispielsweise ist es hierdurch möglich, fälschungssichere Dokumente ohne einen Einsatz von Computern und/oder eine Datenverbindung zu der vertrauenswürdigen Kontaktstelle zu erstellen.

Grundsätzlich ist es möglich, die Schlüsselinformation nach einem vorgegebenen Muster auszuwählen. Dies erleichtert jedoch kryptografische Entschlüsselungsattacken (Enigma-Problem).

Es ist besonders vorteilhaft, dass die Schlüsselinformation dadurch erstellt wird, dass sie zufällig gebildet wird, obwohl die Erfindung mit einem vorgebbaren Satz von Schlüsselinformationen durchgeführt werden kann. Die jeweilige zufällige Erzeugung der Schlüsselinformationen ist deshalb besonders vorteilhaft, da so eine Speicherung einer Vielzahl von Schlüsselinformationen vermieden wird.

Es hat sich als zweckmäßig erwiesen, dass die verschlüsselte Schlüsselinformation und/oder die verschlüsselte Prüfinformation so beschaffen sind, dass sie in der Zwischenstelle nicht entschlüsselt werden können.

Eine Entschlüsselung der Schlüsselinformationen durch das kryptografische Modul beinhaltet mehrere Vorteile. Hierdurch ist es möglich, dass ein Benutzer des kryptografischen Moduls, insbesondere ein Dokumentenhersteller, eine Bestätigung erhält, Informationen der vertrauenswürdigen Kontaktstelle, insbesondere von der vertrauenswürdigen Kontaktstelle geschaffene Geldwerteinformationen erhalten zu haben. Außerdem ist es hierdurch möglich, dass das kryptografische Modul die enthaltene Schlüsselinformation für eine nachfolgende Verschlüsselung einsetzt.

Ein bevorzugter Einsatz der Schlüsselinformationen dient zu einer Verschlüsselung von eigenen Daten des Dokumentherstellers.

Zweckmäßigerweise übergibt der Dokumenthersteller die eigenen Daten in einem möglichst automatisierten Verfahren dem kryptografischen Modul.

Eine besonders bevorzugte Ausführungsform der Erfindung zeichnet sich dadurch aus, dass das kryptografische Modul die vom Dokumenthersteller eingebrachten Daten mit der Schlüsselinformation irreversibel verknüpft.

Hierbei ist es besonders vorteilhaft, dass die irreversible Verknüpfung zwischen den von dem Dokumenthersteller eingebrachten Daten und der entschlüsselten Schlüsselinformation dadurch erfolgt, dass unter Verwendung der Schlüsselinformation ein Prüfwert für das Dokument gebildet wird.

Ferner ist es besonders zweckmäßig, dass das Ergebnis der irreversiblen Verknüpfung der von dem Dokumenthersteller eingebrachten Daten mit der entschlüsselten Schlüsselinformation ein Dokument und/oder einen Datensatz bilden, der an eine Prüfstelle übermittelt wird.

Es hat sich weiter als zweckmäßig erwiesen, dass das an die Prüfstelle übermittelte Dokument die von dem Dokumentersteller eingebrachten eigenen Daten wenigstens teilweise im Klartext enthält.

Dazu ist es besonders zweckmäßig, dass in das an die Prüfstelle übermittelte Dokument die verschlüsselte Prüfinformation eingebracht wird.

Vorteilhaft ist, dass die im kryptografischen Modul verblei-

benden Informationen derart verschlüsselt sind, dass diese im kryptografischen Modul entschlüsselt werden können und dass es sich bei der im kryptografischen Modul verbleibenden Information um einen Wert handelt, der nicht oder nur schwer vorhersagbar ist.

Besonders vorteilhaft ist, dass die Versorgung des kryptografischen Moduls über kryptografisch nicht vertrauenswürdige Kommunikationspartner derart erfolgt, dass ein Austausch von Informationen innerhalb eines Dialogs nicht erforderlich ist.

Ebenfalls von besonderem Vorteil ist, dass die Versorgung des kryptografischen Moduls über kryptografisch nicht vertrauenswürdige Kommunikationspartner derart erfolgt, dass die Weiterreichung der Informationen an das kryptografische Modul zeitlich entkoppelt ist.

Als wichtig und zweckmäßig hat sich ergeben, dass die Versorgung des kryptografischen Moduls auch bei einer Speisung über kryptografisch nicht vertrauenswürdige Kommunikationspartner durch eine vertrauenswürdige Stelle erfolgt, auf deren Informationen sich die Prüfstelle verlassen kann.

Vorteilhaft ist dabei, dass zur Bereitstellung vertrauenswürdiger Informationen für das kryptografische Modul durch eine vertrauenswürdige Stelle kryptografische Verschlüsselungen angewendet werden, die die Prüfstelle rückgängig machen kann.

Eine zweckmäßige Weiterentwicklung des Verfahrens sieht vor, es so durchzuführen, dass die beiden Arten von Daten kryptografisch miteinander verknüpft sind, jedoch nicht auf dem Wege der Kryptoanalyse aufgedeckt werden.

Dazu hat sich als Vorteil gezeigt, dass die kryptografische Verknüpfung der beiden Arten von Daten dergestalt ist, dass

nichtlineare Anteile, die nur der vertrauenswürdigen Kontaktstelle und der Prüfstelle bekannt sind, hinzugefügt werden.

Vorteilhafterweise wird das Verfahren so durchgeführt, dass die erstellten fälschungssicheren Dokumente oder Datensätze geldwerte Informationen enthalten.

Es ist zweckmäßig, dass die geldwerte Information kryptografisch mit dem Dokument oder dem Datensatz derart verbunden ist, dass durch einen Vergleich zwischen der geldwerten Information und dem Dokument oder den Datensatz ein Prüfwert gebildet werden kann.

Ferner ist es vorteilhaft, dass die geldwerten Informationen einen Nachweis über die Entrichtung von Portobeträgen enthalten.

Ein weiterer Vorteil ist darin gegeben, dass die eine Entrichtung eines Portobetrages nachweisenden geldwerte Informationen mit Identifikationsangaben des Dokumentherstellers verknüpft sind.

Ferner ist es nützlich, dass der Nachweis über die Entrichtung eines Portobeitrages mit einer Adressangabe verknüpft ist.

Ein sehr wichtiges Anwendungsgebiet der Erfindung ist die Erzeugung von Freimachungsvermerken. In diesem wesentlichen Anwendungsfall können verschiedene Zwischenstellen eingesetzt werden. Beispielsweise kann ein Wertübertragungszentrum eines Frankiermaschinenherstellers als Zwischenstelle genutzt werden.

Ein weiterer Gegenstand der Erfindung ist ein Wertübertragungszentrum mit einer Schnittstelle zum Laden von Wertbeträgen. In der entsprechenden Weiterentwicklung der Erfindung fungiert das Wertübertragungszentrum vorteilhafterweise als

eine Schnittstelle zum Empfang von verschlüsselten Informationen einer kryptografisch vertrauenswürdigen Kontaktstelle und zur Zwischenspeicherung der empfangenen verschlüsselten Informationen.

Es ist vorteilhaft, dass die Informationen so verschlüsselt sind, dass sie in dem Wertübertragungszentrum nicht entschlüsselt werden können.

Ferner ist es vorteilhaft, dass es Mittel für einen Empfang von Wertübertragungsaufforderungen durch wenigstens ein kryptografisches Modul und zur zeitlich entkoppelten Weitergabe der erhaltenen verschlüsselten Informationen enthält.

Besonders vorteilhaft ist ein kryptografisches Modul zur Erzeugung fälschungssicherer Dokumente mit Mitteln zur Ausgabe von verschlüsselten Prüfinformationen und eines Prüfwerts.

Eine vorteilhafte Ausführungsform sieht vor, dass das kryptografische Modul wenigstens ein Mittel zum Empfang und zur Entschlüsselung von Schlüsselinformationen und wenigstens ein Mittel zum Empfang eines Dokuments oder eines Datensatzes enthält, und dass das kryptografische Modul über wenigstens ein Mittel zur Erstellung eines Prüfwerts für das Dokument oder den Datensatz verfügt.

Weitere Vorzüge, Besonderheiten und zweckmäßige Weiterbildungen der Erfindung ergeben sich aus den Unteransprüchen und der nachfolgenden Darstellung bevorzugter Ausführungsbeispiele anhand der Zeichnungen.

Von den Zeichnungen zeigt

Fig. 1 das Grundprinzip eines bekannten kryptografischen Verfahrens,

Fig. 2 eine Prinzipskizze für eine Prinzipdarstellung einer erfindungsgemäßen Erzeugung digitaler Freimachungen und

Fig. 3 eine Prinzipdarstellung besonders bevorzugter Verfahrensschritte für die Erzeugung fälschungssicherer Dokumente.

Zur Lösung dieses Problems ist aus der Deutschen Patentschrift DE 100 20 563 C2 ein Verfahren zur Erstellung fälschungssicherer Dokumente bekannt, bei dem die Notwendigkeit, Informationen aus dem kryptografischen Modul des Dokumentherstellers zur Prüfung zu verwenden, entfällt. Statt dessen basiert dieses Verfahren darauf, dass eine Zufallszahl im kryptografischen Modul des Kunden gebildet wird. Das genaue Verfahren mit seinen drei beteiligten Parteien (1. Dokumentherstellen mit kryptografischem Modul, 2. Prüfstelle und 3. Vertrauenswürdige Kontaktstelle) ist in der beigefügten Fig. 1 dargestellt. Die im nachfolgenden Text genannten Nummern beziehen sich auf die in der Fig. 1 dargestellten Schritte des Verfahrens.

In Fig. 1 wird im kryptografischen Modul des Dokumentherstellers eine Zufallszahl erzeugt und gespeichert (1), die zusammen mit der Identität oder Identifikationsnummer des Dokumentherstellers oder des kryptografischen Moduls verschlüsselt (2) an eine vertrauenswürdige Stelle übermittelt wird (3). Diese vertrauenswürdige Stelle entschlüsselt die Zufallszahl und die Identifikationsnummer (4), überprüft die Rechtmäßigkeit der Anfrage (5) und verschlüsselt daraufhin die Zufallszahl und einen neu gebildeten Transaktions-Indikator in der Weise, dass nur die Prüfstelle in der Lage ist, diese Verschlüsselung rückgängig zu machen (6). Die derart verschlüsselte Zufallszahl und der Transaktions-Indikator

werden an den Dokumenthersteller zurückgesandt (7). Bei der späteren Erzeugung fälschungssicherer Dokumente gibt der Dokumenthersteller nun das zu sichernde Dokument in das kryptografische Modul ein (8). Dort wird unter Verwendung des Dokumenten-Klartextes und der noch immer gespeicherten Zufallszahl ein Prüfwert gebildet (9). Übertragen zur Prüfstelle wird nun das Dokument im Klartext, die von der vertrauenswürdigen Stelle übertragene verschlüsselte Zufallszahl und der verschlüsselte Transaktionsindikator sowie die im kryptografischen Modul erzeugte Prüfinformation (10). In der Prüfstelle erfolgt die Feststellung der Unverfälschtheit nach einer Grobprüfung der Dokumentenstruktur (11) durch Entschlüsselung der Zufallszahl und des Transaktions-Indikators, die in der vertrauenswürdigen Kontaktstelle verschlüsselt worden waren (12). Anschließend wird wie im kryptografischen Modul des Dokumentherstellers unter Verwendung des Dokumenten-Klartexts und der soeben entschlüsselten Zufallszahl ein Prüfwert gebildet (13). Dieser Prüfwert wird schließlich mit dem vom Dokumenthersteller übertragenen Prüfwert verglichen (14). Stimmen beide überein, so ist sichergestellt, dass das Dokument unter Verwendung eines bestimmten kryptografischen Moduls erzeugt wurde, da die erforderliche Zufallszahl nur dort vorhanden ist und dieses Modul kryptografisch abgesichert mit der vertrauenswürdigen Kontaktstelle Informationen ausgetauscht hat. Da zum einen ein bestimmtes kryptografisches Modul verwendet wurde und zum anderen der Prüfwert übereinstimmt, ist sowohl die Identität des Dokumentherstellers als auch die Unverfälschtheit des Dokuments sichergestellt.

Das beschriebene Verfahren wird in Abwandlung von der Deutschen Post für die Herstellung von Internet-Briefmarken unter der Bezeichnung „PC-Frankierung" eingesetzt. Es zeichnet sich zusammengefasst dadurch aus, dass die Prüfung der Unverfälschtheit der Dokumente ohne Benutzung von Schlüsselinfor-

mationen erfolgen kann, die dem kryptografischen Modul eigen sind. Vielmehr verlässt sich die Prüfstelle zum Teil auf Informationen einer vertrauenswürdigen Kontaktstelle.

Erfindungsgemäß wird ein Verfahren zur Erzeugung digitaler Dokumente und Datensätze geschaffen, das ohne einen direkten Kontakt zwischen einer kryptografisch vertrauenswürdigen Kontaktstelle und dem kryptografischen Modul, beziehungsweise einem das kryptografische Modul einsetzenden Dokumentenhersteller erfolgen kann.

Obwohl die Erzeugung der Dokumente und Datensätze keineswegs auf die Erzeugung von Freimachungsvermerken, beziehungsweise auf mit Freimachungsvermerke versehene Postsendungen beschränkt ist, stellt der Einsatz der dargestellten Verfahrens- und Vorrichtungsmerkmale in einem Verfahren zur Erzeugung digitaler Freimachungen eine besonders bevorzugte Ausführungsform der Erfindung dar.

Eine derartige Ausführungsform wird nachfolgend anhand von Fig. 2 dargestellt.

Das schematische Modell beziehungsweise die Funktionsweise der neuen digitalen Freistempelung ist in FIG. 2 skizziert und nachfolgend beschrieben:

1. Im ***Vorfeld*** des Ladevorgangs zwischen dem Vorgabezentrum des Anbieters und der Digitalen Freistempelmaschine des Kunden stellt das Postunternehmen dem Anbieter auf elektronischem Wege ***maschinenbezogene Informationen*** zur zukünftigen Einspeisung in die Digitalen Freistempelmaschinen zur Verfügung. Diese Informationen umfassen unter anderem eine Schlüsselinformation zur Verwendung in der Maschine und einen sogenannten „ValidityString", der zur späteren

Prüfung im Briefzentrum verwendet wird sowie Informationen zur Bonität von Kunden. Teile dieser Informationen sind derart verschlüsselt, dass sie nur innerhalb der Freistempelmaschine entschlüsselt werden können.

2. Zwischen der Digitalen Freistempelmaschine des Kunden und dem Fernwähl-Vorgabezentrum des Herstellers wird ein ***Vorgabe-Ladevorgang*** mit dem Ziel durchgeführt, den verfügbaren Portowert in der Freistempelmaschine zu erhöhen. Während dieses Ladevorgangs werden auch die (zuvor von der Deutschen Post bereitgestellten) maschinenbezogenen Informationen in einen manipulationssicheren Bereich der Digitalen Freistempelmaschine übertragen. Ein derartiger Ladevorgang, bei dem die (von dem Postunternehmen bereitgestellten) Informationen in die Maschine übertragen werden, sollte innerhalb bestimmter Toleranzen regelmäßig, beispielsweise einmal innerhalb eines vorgebbaren Zeitintervalls, beispielsweise monatlich erfolgen. Falls keine neue Vorgaben geladen werden sollen, ist einmal monatlich ein entsprechender Kommunikationsvorgang zwischen der Freistempelmaschine und dem Vorgabezentrum durchzuführen, bei dem ebenfalls die von dem Postunternehmen bereitgestellten Informationen in die Maschine übertragen werden. Die Kommunikation zwischen Vorgabezentrum und Digitaler Freistempelmaschine muss in angemessener und überprüfbarer Weise abgesichert sein.

3. Im Nachgang des Vorgabe-Ladevorgangs (Schritt 1.) findet zwischen dem Vorgabezentrum des Anbieters und dem als vertrauenswürdige Kontaktstelle dienenden Postage-Point des Postunternehmens eine gesicherte, elektronische Kommunikation über den ***Kauf eines bestimmten Portobetrags für einen Kunden*** statt. Bei dieser Datenübertragung werden Abrechnungs- und Nutzungsinformationen an das Postunternehmen übertragen. Da die oben beschriebene Bereitstellung von Informationen für den nächsten Ladevorgang deutlich im voraus erfolgen kann, ist es möglich, aber nicht notwendig, die Schritte 3 und 1 zu kombinieren, sodass Schritt 3

des soeben abgeschlossenen Ladevorgangs mit Schritt 1 für den nachfolgenden Ladevorgang zusammentreffen.

4. Den bei der vertrauenswürdigen Kontaktstelle, dem Postage-Point des Postunternehmens, gekauften Portobetrag stellt das Postunternehmen dem Kunden unmittelbar per Lastschrift in ***Rechnung***.

5. Mit der geladenen Digitalen Freistempelmaschine können prinzipiell so lange gültige ***digitale Freistempelabdrucke ausgedruckt*** werden, bis das Guthaben aufgebraucht ist. Die digitalen Freistempelabdrucke enthalten einen zweidimensionalen Matrixcode (2D-Barcode), in dem zusätzliche Daten enthalten sind, die unter anderem, wie in Schritt 1 beschrieben, im Vorfeld von dem Postunternehmen zur Verfügung gestellt wurden und die im Briefzentrum zur Prüfung der Gültigkeit herangezogen werden.

6. Postsendungen mit digitalem Freistempelabdruck können über die von dem Postunternehmen bereitgestellten Möglichkeiten, z.B. Briefkasten, Postfiliale, eingeliefert werden.

7. Sendungen mit digitalem Freistempelabdruck werden von dem Postunternehmen nach Überprüfung der Gültigkeit befördert.

8. In einem Abgleich können geladene Portowerte des Kunden mit den im Briefzentrum gelesenen Portowerten verglichen werden.

Bei den Informationen, die, wie im o.g. Schritt 1 beschrieben, vorab von der Deutschen Post zur Verfügung gestellt werden, sind im Sinne der vorliegenden Erfindung zwei Bestandteile von Bedeutung, nämlich zum einen eine Schlüsselinformation m_{key} zur Verwendung in der Maschine und zum anderen eine sogenannte Prüfinformation VS. Die Schlüsselinformation m_{key} wird vom Postage Point des Postunternehmens, der als vertrauenswürdige Kommunikationsstelle dient, derart verschlüsselt, dass eine Entschlüsselung nur im manipulationssicheren Be-

reich der Digitalen Freistempelmaschine (kryptografisches Modul) möglich ist. Die in sich bereits verschlüsselte Prüfinformation VS kann ohne weitere Transportverschlüsselung an die Freistempelmaschine bzw. das kryptografische Modul übertragen werden. Durch die Verschlüsselung der Schlüsselinformation m_{key} ist eine Entschlüsselung nur im kryptografischen Modul der Freistempelmaschine möglich, nicht jedoch auf dem nicht vertrauenswürdigen Kommunikationsweg.

Das Prinzip der Sicherheit der Erstellung fälschungssicherer Dokumente mit einem extern auf unsicherem Weg gespeisten kryptografischen Modul wird in der FIG. 3 schematisch dargestellt:

1. In einem ersten Schritt wird in einer vertrauenswürdigen Kontaktstelle, die in der praktischen Realisierung dem Postage Point des Postunternehmens entspricht, eine **Schlüsselinformation** gebildet. Diese Schlüsselinformation dient später dazu, im kryptografischen Modul zur Erstellung eines Prüfwerts herangezogen zu werden. Sinnvollerweise verbleibt diese Schlüsselinformation später im kryptografischen Modul und wird dieses nicht verlassen.

2. In einem zweiten Schritt wird eine sogenannte Prüfinformation gebildet. Diese wird zusammengestellt aus der Schlüsselinformation aus Schritt 1, einem Transaktions-Indikator, der Zusatzinformationen zum nächsten Ladevorgang des Kunden enthält, sowie aus weiteren Informationen. Die Zusammenstellung und anschließende Verschlüsselung dieser Elemente der Prüfinformation geschieht in einer Weise, dass nur die Prüfstelle später in der Lage ist, diese Verschlüsselung wieder rückgängig zu machen. Die Zusammenstellung und anschließende Verschlüsselung dieser Elemente der Prüfinformation geschieht außerdem in einer Weise, dass auch mit Kenntnis der Schlüsselinformationen im Klartext, was jedoch theoretisch außerhalb der vertrauenswür-

digen Kontaktstelle und außerhalb des kryptografischen Moduls kaum möglich ist, eine Aufdeckung des Schlüssels zur Verschlüsselung der Prüfinformationen zur anschließenden Entschlüsselung an der Prüfstelle vermieden wird.

3. In einem dritten Schritt werden die im ersten Schritt erzeugten Schlüsselinformationen derart verschlüsselt, dass eine Entschlüsselung nur im kryptografischen Modul beim Dokumenthersteller erfolgen kann, nicht jedoch auf dem Übertragungsweg dorthin.

4. In einem vierten Schritt werden nun, vorzugsweise zusammen mit anderen, die Manipulationssicherheit weiter erhöhenden Informationen zum anstehenden Ladevorgang des Kunden, die zwei Arten von Informationen übergeben. Zum einen handelt es sich dabei um die in Schritt 1 erstellte und in Schritt 3 verschlüsselte Schlüsselinformation, die später in das kryptografische Modul geladen, dort entschlüsselt wird und dort auch zur Erstellung fälschungssicherer Dokumente verbleibt. Zum anderen handelt es sich dabei um die in Schritt 2 gebildete verschlüsselte Prüfinformation, die nur von der Prüfstelle wieder entschlüsselt werden kann und die an jedes vom Dokumenthersteller später erzeugte Dokument angehängt wird.

5. In einem fünften Schritt werden die zwei Arten von Informationen, die im Rahmen dieser Erfindung relevant sind, zusammen mit anderen Informationen zum anstehenden Ladevorgang des Kunden in der nicht vertrauenswürdigen Stelle zwischengespeichert. Eine Entschlüsselung der beiden relevanten Arten von Informationen ist an dieser Stelle nicht möglich. Insbesondere ist eine Aufdeckung des Schlüssels, der in der vertrauenswürdigen Stelle verwendet wurde, um die Prüfinformationen derart zu verschlüsseln, dass nur die Prüfstelle diese wieder entschlüsseln kann, schon deshalb nicht möglich, weil der Klartext der Schlüsselinformation, der für eine solche sogenannte Klartextattacke notwendig wäre, nicht vorliegt.

6. In einem sechsten Schritt werden die von der vertrauenswürdigen Stelle zur Verfügung gestellten Informationen zeitlich entkoppelt, z.B. im Rahmen des nächsten Ladevorgangs, an das kryptografische Modul beim Dokumenthersteller übergeben.

7. Der siebte Schritt weist auf die Kommunikation zwischen nicht vertrauenswürdiger Stelle und kryptografischem Modul hin, die vorzugsweise durch zusätzliche geeignete Mittel kryptografisch abgesichert ist. Immerhin handelt es sich in der praktischen Realisierung um die Kommunikation zwischen einem Vorgabezentrum eines Herstellers und dessen Freistempelmaschine mit kryptografischem Modul, die schon wegen des elektronisch ausgetauschten Ladebetrags gegen Manipulationen geschützt werden muss. Wäre diese Kommunikation nicht geschützt, so wäre eine unberechtigte Erhöhung des Ladebetrags möglich. Nur im Sinne dieser Erfindung gilt daher das Vorgabezentrum des Herstellers als „nicht vertrauenswürdige" Stelle, in der praktischen Realisierung ist das Vorgabezentrum durchaus als vertrauenswürdig einzustufen.

8. Im achten Schritt findet eine Entschlüsselung und anschließende Speicherung der Schlüsselinformation statt, die in Schritt 3 verschlüsselt wurde. Diese Schlüsselinformation wird später benutzt, um Dokumente durch Erstellung eines Prüfwerts abzusichern. Zur Vermeidung von oben bereits erwähnten Klartext-Attacken ist es wichtig, dass die Schlüsselinformation nicht aus dem kryptografischen Modul ausgelesen werden kann, sondern nur innerhalb des Moduls durch ebenfalls beinhaltete Prozesse verwendet wird.

9. In einem neunten Schritt wird die verschlüsselte Prüfinformation aus Schritt 2 gespeichert. Da diese Information bereits verschlüsselt ist und nicht weiter im kryptografischen Modul zur Datenverarbeitung benötigt wird, ist ihre Speicherung außerhalb des kryptografischen Moduls

möglich. Die verschlüsselte Prüfinformation wird später an jedes gesicherte Dokument angehängt, um in der Prüfstelle verwendet zu werden.

10. In einem zehnten, vorzugsweise zeitlich entkoppelten Schritt gibt der Kunde bzw. Dokumenthersteller die Inhalte des zu sichernden Dokuments in das kryptografische Modul ein.

11. In einem elften Schritt wird mit den eingegebenen Klartextinformationen des Dokuments unter Verwendung der noch gespeicherten Schlüsselinformation aus Schritt 1 ein Prüfwert gebildet. Die Bildung des Prüfwerts findet durch Anwendung eines üblichen Prüfwert-Verfahrens statt, wie z.B. MAC, HMAC symmetrische Signatur o.ä.. Mehreren besonders bevorzugten Ausführungsformen ist gemein, dass der Klartext des Dokuments in der Regel irreversibel verkürzt und gleichzeitig oder anschließend mit einem Schlüssel, in diesem Falle der Schlüsselinformation aus Schritt 1, verschlüsselt wird.

12. In einem zwölften Schritt wird nun das Dokument übertragen. Das Gesamtdokument besteht dabei vorzugsweise aus mehreren, insbesondere drei Bestandteilen. Ein erster Bestandteil ist die eigentliche Klartextinformation des Dokuments.
Als zweiter Bestandteil des Gesamtdokuments sind an den Dokumententext die verschlüsselten Prüfinformationen aus Schritt 2 angehängt, die in Schritt 9 im kryptografischen Modul oder außerhalb des Moduls gespeichert wurden und fortan jedem zu sichernden Dokument beigefügt werden.
Als dritter Bestandteil des Gesamtdokuments ist der in Schritt 11 gebildete Prüfwert angehängt.

13. Im dreizehnten Schritt erreicht das Dokument die Prüfstelle, wo es auf strukturelle Vollständigkeit und Unversehrtheit geprüft wird. In der konkreten Anwendung der Erfindung zur Prüfung von Freimachungsvermerken können an dieser Stelle auch weitere Schlüssigkeitsprüfungen statt-

finden. Da in diesem Falle das gesicherte Dokument dem maschinenlesbaren Frankiervermerk entspricht, kann dieser gegen andere Sendungsinformationen wie Anschrift und Sendungsart sowie allgemeine Informationen wie das Datum geprüft werden. Hierdurch kann ausgeschlossen werden, dass ein in sich gültiger Frankiervermerk zur Freimachung einer nicht zu diesem Frankiervermerk passenden Sendung verwendet wird.

14. Im vierzehnten Schritt wird die in Schritt 2 verschlüsselte Prüfinformation wieder entschlüsselt. Die aus mehreren Komponenten zusammengesetzte Prüfinformation wird wieder in ihre Bestandteile zerlegt. Neben anderen Informationen werden dabei insbesondere die Schlüsselinformation und der Transaktions-Indikator gewonnen. Letzterer kann einer zusätzlichen Prüfung dienen. So kann beispielsweise die im Transaktions-Indikator hinterlegte Identität des Kunden bzw. Dokumentherstellers mit einer in der Prüfstelle hinterlegten Positivliste erwünschter Dokumentenhersteller oder einer Negativliste unerwünschter Dokumentenhersteller verglichen werden.

15. In einem fünfzehnten Schritt wird in Analogie zu Schritt 11 ein Prüfwert erstellt. Nach dem gleichen Verfahren wie bei Schritt 11 werden nun die in der Prüfstelle vorliegenden Klartextinformationen des Dokuments unter Verwendung der soeben entschlüsselten Schlüsselinformation aus Schritt 14 ein Prüfwert gebildet. Können verschiedene Verfahren zur Erstellung von Prüfwerten im kryptografischen Modul möglich sein, so muss die konkrete Wahl des Verfahrens ebenfalls angehängt an das Dokument oder im Dokument vom Dokumentenhersteller an die Prüfstelle übertragen werden.

16. Im abschließenden Schritt sechzehn wird der im kryptografischen Modul erstellte und an das Dokument angehängte Prüfwert mit dem in der Prüfstelle erstellten Prüfwert verglichen. Nur wenn beide Prüfwerte übereinstimmen,

ist gewährleistet, dass das Dokument unter Verwendung des kryptografischen Moduls beim Dokumentherstellers erstellt wurde.

Ein in missbräuchlicher Absicht agierender Dokumentherstellers, der ein gesichertes Dokument eines Kunden vortäuschen will, jedoch nicht Zugriff auf dessen kryptografisches Modul hat, wird nicht in der Lage sein, die Schlüsselinformation aus Schritt 1 zu erhalten und zu entschlüsseln. Diese ist jedoch unabdingbar, um einen Prüfwert herzustellen, der mit dem in der Prüfstelle hergestellten übereinstimmt. Erfindet ein in missbräuchlicher Absicht agierender Dokumenthersteller hingegen eine geeignete Schlüsselinformation, die er auch sinngemäß korrekt zur Bildung eines Prüfwerts anwenden kann, so gelingt es ihm nicht, eine hierzu passende verschlüsselte Prüfinformation herzustellen. Diese verschlüsselte Prüfinformation müsste derart verschlüsselt sein, dass nur die Prüfstelle in der Lage ist, eine Entschlüsselung vorzunehmen. Ohne Kenntnis der verwendeten Schlüssel ist dies nicht möglich. Folglich ist das System sicher und nicht überwindbar.

Durch die Erfindung ist es möglich, fälschungssichere Dokumente zu erzeugen und die Unverfälschtheit der in dem Dokument enthaltenen Daten und/oder die Identität des Dokumentherstellers zuverlässig zu prüfen.

Alle hierzu erforderlichen Prüfinformationen werden vorzugsweise durch die vertrauenswürdige Kontaktstelle und/oder das kryptografische Modul zur Verfügung gestellt.

Die Erfindung eignet sich für eine Erzeugung beliebiger Dokumente. Es ist jedoch besonders vorteilhaft, die Erfindung für eine Erzeugung digitaler Dokumente einer verhältnismäßig geringen Datenmenge in der Größenordnung von wenigen Bit bis zu Dokumenten mit einer Gesamtgröße einschließlich Prüfinformationen bis etwa 60 byte einzusetzen.

Besonders bevorzugte Dokumente im Sinne der Erfindung sind Gültigkeitsvermerke für eine Vielzahl von Anwendungsgebieten. Es ist besonders vorteilhaft, die Erfindung für eine Überprüfung digitaler Freimachungsvermerke für Postsendungen einzusetzen, da sie eine besonders schnelle und einfache Erzeugung der Freimachungsvermerke ermöglicht. Ein Einsatz für andere Gebiete als Nachweis für die Entrichtung von Geldbeträgen - digitale Wertmarken -, beziehungsweise als sonstiger Träger einer Geldwertinformation ist gleichfalls möglich.

Die Erfindung eignet sich insbesondere für alle Anwendungsfälle, bei denen außer dem Dokumentersteller wenigstens eine Prüfinstanz ein Interesse an der Unverfälschtheit des Dokuments haben. Die Erfindung eignet sich hierdurch für weite Anwendungsbereiche, insbesondere für die Erstellung von digitalen Wertmarken für eine Vielzahl von Einsatzgebieten, beispielsweise als Flugtickets, Fahrkarten, Theater- oder Kinokarten. Derartige Dokumente können mit Hilfe der Erfindung von dem Dokumenthersteller selber ausgedruckt werden, wobei es möglich ist, dass der Dokumenthersteller hierzu vorhandene Guthaben - oder Kreditbeträge - ausnutzt und auf diese Weise einen zuverlässigen Beweis der Zahlung erhält.

Das Erzeugen dieser Dokumente kann beispielsweise über einen herkömmlichen Personalcomputer oder einen kryptografisch nicht gesicherten Drucker erfolgen. Ein besonderer Vorteil der Erfindung ist, dass die Erstellung der Dokumente ohne eine Verbindung zwischen der Erzeugung der Dokumente ohne direkte Verbindung zwischen dem Dokumenthersteller und der vertrauenswürdigen Kontaktstelle erfolgen kann. Die Dokumentherstellung ist hierdurch auch bei Zwischenschaltung einer oder mehrerer Zwischenstellen, beziehungsweise bei einer Kommunikation über kryptografisch nicht oder nur schwer sicherbare Datenwege möglich.

Die kryptografisch vertrauenswürdige Kontaktstelle und/oder die Prüfstelle erhalten Mittel um sicherzustellen, dass keine unberechtigten Dokumente erzeugt wurden, beziehungsweise dass keine Dokumente verfälscht wurden. Hierdurch ist es auf eine besonders einfache und zuverlässige Weise möglich, prüfbar sichere digitale Dokumente zu erzeugen und diese Dokumente zuverlässig zu überprüfen.

Eine derartige Prüfung kann auf verschiedene Weisen erfolgen, wobei die genannten kryptografischen Verfahrensschritte einfach und zuverlässig angewendet werden können. Hierdurch ist ein Einsatz der Erfindung außerhalb der besonders bevorzugten Überprüfung der Echtheit digitaler Freimachungen von Postsendungen, beispielsweise durch eine Überprüfung der Echtheit der digitalen Fahrkarten, Flugtickets ect. durch einen Kontrolleur, beziehungsweise bei einer Einlasskontrolle, möglich.

Die dargestellten erfindungsgemäßen Mittel und Verfahrensschritte können auch auf Dokumente angewendet werden, die vor oder während der Erstellung der Fälschungssicherheit im Sinne dieser Erfindung ebenfalls verschlüsselt werden. In diesem Fall wird das Verfahren vorzugsweise nicht auf einen unverschlüsselten Klartext, sondern einen verschlüsselten Text angewandt, wobei sich jedoch die Verfahren dieser Erfindung nicht unterscheiden. Je nach Ausprägungsform wäre es gleichfalls möglich, dass die Verschlüsselung ebenfalls im kryptografischen Modul erfolgt und somit nach Darstellung in Fig. 3 ein Zwischenschritt der Verschlüsselung zwischen den hier geschilderten Schritten zehn und elf erfolgen würde.

Patentansprüche:

1. Verfahren zur Erstellung fälschungssicherer Dokumente oder Datensätze, wobei eine Schlüsselinformation erzeugt wird und wobei eine verschlüsselte Prüfinformation aus der Schlüsselinformation und einem Transaktionsindikator gebildet wird, d a d u r c h g e k e n n z e i c h n e t, dass die Erstellung der zufälligen Schlüsselinformation und die Bildung der verschlüsselten Prüfinformation aus der Schlüsselinformation und dem Transaktionsindikator in einer kryptografisch vertrauenswürdigen Kontaktstelle erfolgen, dass die kryptografisch vertrauenswürdige Kontaktstelle die Schlüsselinformation verschlüsselt, und dass die verschlüsselte Prüfinformation und die verschlüsselte Schlüsselinformation von der kryptografisch vertrauenswürdigen Kontaktstelle an eine Zwischenstelle übermittelt werden, dass die Zwischenstelle die verschlüsselte Schlüsselinformation und die verschlüsselte Prüfinformation zwischenspeichert und zu einem späteren Zeitpunkt zeitlich von der Übertragung zwischen der kryptografisch vertrauenswürdigen Kontaktstelle und der Zwischenstelle entkoppelt an ein kryptografisches Modul eines Dokumentherstellers übermittelt.

2. Verfahren nach Anspruch 1, d a d u r c h g e k e n n z e i c h n e t, dass die Schlüsselinformation so erstellt wird, dass die Schlüsselinformation zufällig gebildet wird.

3. Verfahren nach einem oder mehreren der vorangegangenen Ansprüche, d a d u r c h g e k e n n z e i c h n e t, dass die verschlüsselte Schlüsselinformation und/oder die verschlüsselte Prüfinformation so beschaffen sind, dass sie in der Zwischenstelle nicht entschlüsselt werden können.

4. Verfahren nach einem oder mehreren der vorangegangenen Ansprüche, d a d u r c h g e k e n n z e i c h n e t, dass das kryptografische Modul vorzugsweise mit einem in dem kryptografischen Modul enthaltenen Schlüssel eine Entschlüsselung der Schlüsselinformation vornimmt.

5. Verfahren nach einem oder mehreren der vorangegangenen Ansprüche, d a d u r c h g e k e n n z e i c h n e t, dass der Dokumenthersteller eigene Daten dem kryptografischen Modul übergibt.

6. Verfahren nach einem oder mehreren der vorangegangenen Ansprüche, d a d u r c h g e k e n n z e i c h n e t, dass das kryptografische Modul die vom Dokumenthersteller eingebrachten Daten mit der Schlüsselinformation irreversibel verknüpft.

7. Verfahren nach Anspruch 6, d a d u r c h g e k e n n z e i c h n e t, dass die irreversible Verknüpfung zwischen den von dem Dokumenthersteller eingebrachten Daten und der entschlüsselten Schlüsselinformation dadurch erfolgt, dass unter Verwendung der Schlüsselinformation ein Prüfwert für das Dokument gebildet wird.

8. Verfahren nach einem oder beiden der Ansprüche 6 oder 7, d a d u r c h g e k e n n z e i c h n e t, dass das Ergebnis der irreversiblen Verknüpfung der von dem Dokumenthersteller eingebrachten Daten mit der entschlüsselten Schlüsselinformation ein Dokument und/oder einen Datensatz bilden, der an eine Prüfstelle übermittelt wird.

9. Verfahren nach Anspruch 8, d a d u r c h g e k e n n z e i c h n e t, dass das an die Prüfstelle übermittelte Dokument die von dem Dokumenthersteller eingebrachten eigenen Daten wenigstens teilweise im Klartext enthält.

10. Verfahren nach einem oder beiden der Ansprüche 8 oder 9, dadurch gekennzeichnet, dass in das an die Prüfstelle übermittelte Dokument die verschlüsselte Prüfinformation eingebracht wird.

11. Verfahren nach einem oder mehreren der vorangegangenen Ansprüche, dadurch gekennzeichnet, dass in dem kryptografischen Modul Informationen verbleiben, die derart verschlüsselt sind, dass sie im kryptografischen Modul entschlüsselt werden können.

12. Verfahren nach einem oder mehreren der vorangegangenen Ansprüche, dadurch gekennzeichnet, dass die Versorgung des kryptografischen Moduls mit den Informationen auch bei einer Speisung über im kryptografischen Sinne nicht vertrauenswürdige Kommunikationspartner durch eine kryptografisch vertrauenswürdige Stelle erfolgt, auf deren Information sich die Prüfstelle verlassen kann.

13. Verfahren nach Anspruch 12, dadurch gekennzeichnet, dass zur Bereitstellung vertrauenswürdiger Informationen für das kryptografische Modul durch eine vertrauenswürdige Stelle kryptografische Verschlüsselungen angewendet werden, die die Prüfstelle rückgängig machen kann.

14. Verfahren nach einem oder mehreren der Ansprüche .. bis 13, dadurch gekennzeichnet, dass die Versorgung des kryptografischen Moduls über kryptografisch nicht vertrauenswürdige Kommunikationspartner derart erfolgt, dass die Weiterreichung der Informationen an das kryptografische Modul zeitlich entkoppelt ist.

15. Verfahren nach einem oder mehreren der Ansprüche 1 bis 14, dadurch gekennzeichnet, dass die Versorgung des kryptografischen Moduls über kryptogra-

fisch nicht vertrauenswürdige Kommunikationspartner derart erfolgt, dass ein Austausch von Informationen innerhalb eines Dialogs nicht erforderlich ist.

16. Verfahren nach einem oder mehreren der Ansprüche 1 bis 14, dadurch gekennzeichnet, dass die beiden Arten von Daten kryptografisch miteinander verknüpft sind, jedoch nicht auf dem Wege der Kryptoanalyse aufgedeckt werden.

17. Verfahren nach Anspruch 16, dadurch gekennzeichnet, dass die kryptografische Verknüpfung der beiden Arten von Daten dergestalt ist, dass nicht lineare Anteile, die nur der vertrauenswürdigen Kontaktstelle und der Prüfstelle bekannt sind, hinzugefügt werden.

18. Verfahren nach einem oder mehreren der vorangegangenen Ansprüche, dadurch gekennzeichnet, dass die erstellten fälschungssicheren Dokumente oder Datensätze Geldwerteinformationen enthalten.

19. Verfahren nach 18, dadurch gekennzeichnet, dass die Geldwerteinformation kryptografisch mit dem Dokument oder dem Datensatz derart verbunden ist, dass durch einen Vergleich zwischen den Geldwerteinformationen und dem Dokument oder den Datensatz ein Prüfwert gebildet werden kann.

20. Verfahren nach einem oder beiden der Ansprüche 18 oder 19, dadurch gekennzeichnet, dass die Geldwerteinformationen einen Nachweis über die Entrichtung von Portobeträgen enthalten.

21. Verfahren nach Anspruch 20, dadurch gekennzeichnet, dass die den Entrichtung des Portobetrages nachweisenden geldwerter Informationen mit

Identifikationsangaben des Dokumentherstellers verknüpft sind.

22. Verfahren nach einem oder beiden der Ansprüche 20 oder 21, dadurch gekennzeichnet, dass die geltwerten Informationen mit einer Adressangabe verknüpft werden.

23. Wertübertragungszentrum mit einer Schnittstelle zum Laden von Wertbeträgen, dadurch gekennzeichnet, dass das Wertübertragungszentrum eine Schnittstelle zum Empfang von verschlüsselten Informationen einer kryptografisch vertrauenswürdigen Kontaktstelle und zur Zwischenspeicherung der empfangenen verschlüsselten Informationen enthält.

24. Wertübertragungszentrum nach Anspruch 23, dadurch gekennzeichnet, dass die Informationen so verschlüsselt sind, dass sie in dem Wertübertragungszentrum nicht entschlüsselt werden können.

25. Wertübetragungszentrum nach einem oder mehreren der Ansprüche 23 bis 24, dadurch gekennzeichnet, dass es Mittel für einen Empfang von Wertübertragungsaufforderungen durch wenigstens ein kryptografisches Modul und zur zeitlich entkoppelten Weitergabe der erhaltenen verschlüsselten Informationen enthält.

26. Kryptografisches Modul zur Erzeugung fälschungssicherer Dokumtente mit Mitteln zur Ausgabe von verschlüsselten Prüfinformationen und eines Prüfwerts, dadurch gekennzeichnet, dass das kryptografische Modul wenigstens ein Mittel zum Empfang und zur Entschlüsselung von Schlüsselinformationen und wenigstens ein Mittel zum Empfang eines Dokuments oder eines Datensatzes enthält, und dass das kryptografische Modul wenigstens

ein Mittel zur Erstellung eines Prüfwerts für das Dokument oder den Datensatz unter Verwendung der Schlüsselinformation enthält.

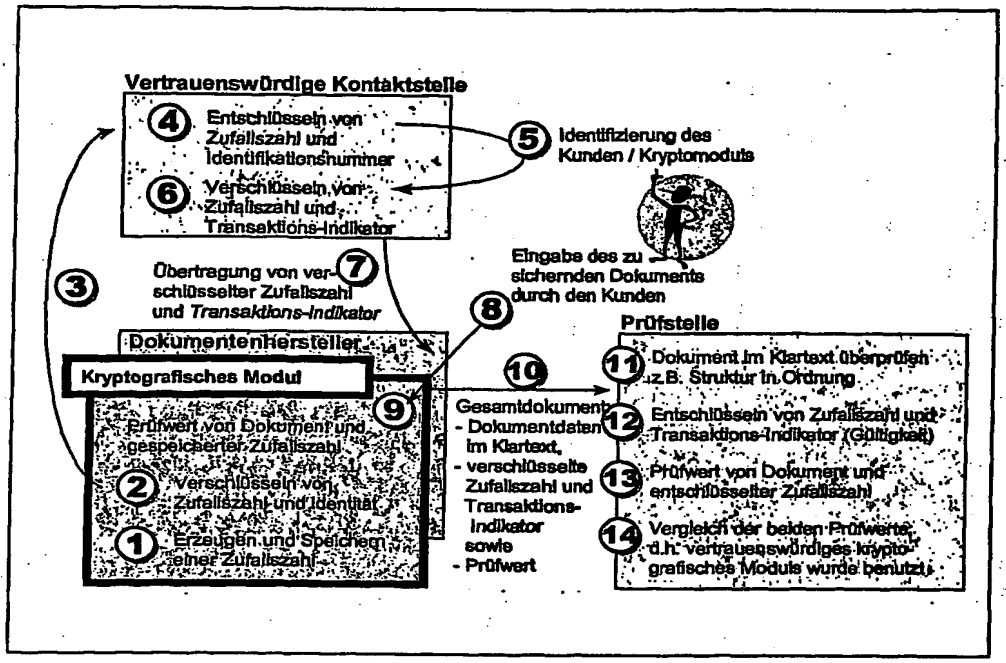

FIG. 1

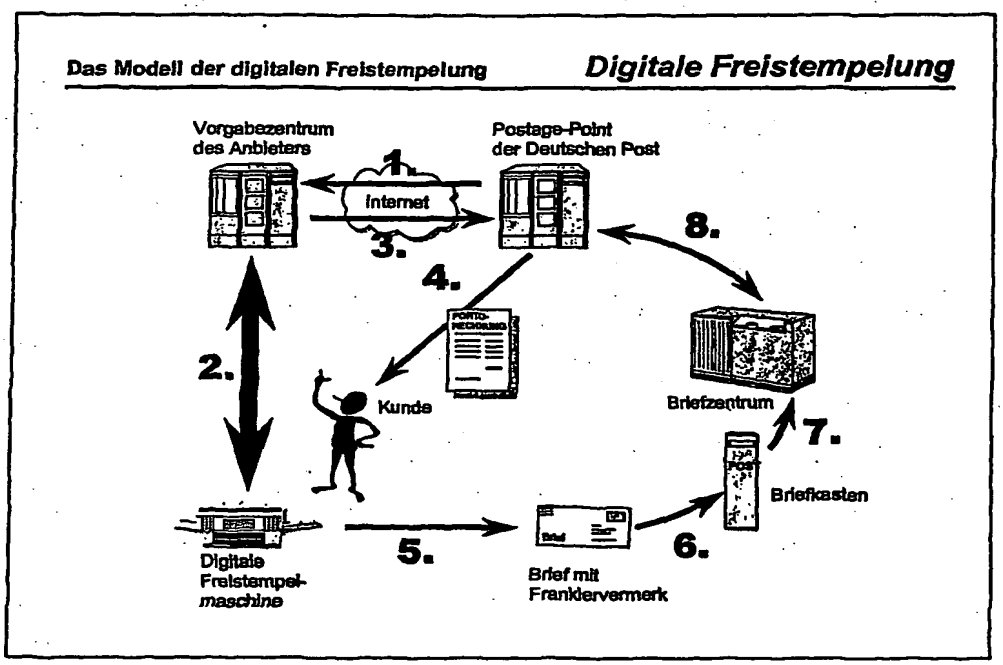

FIG. 2

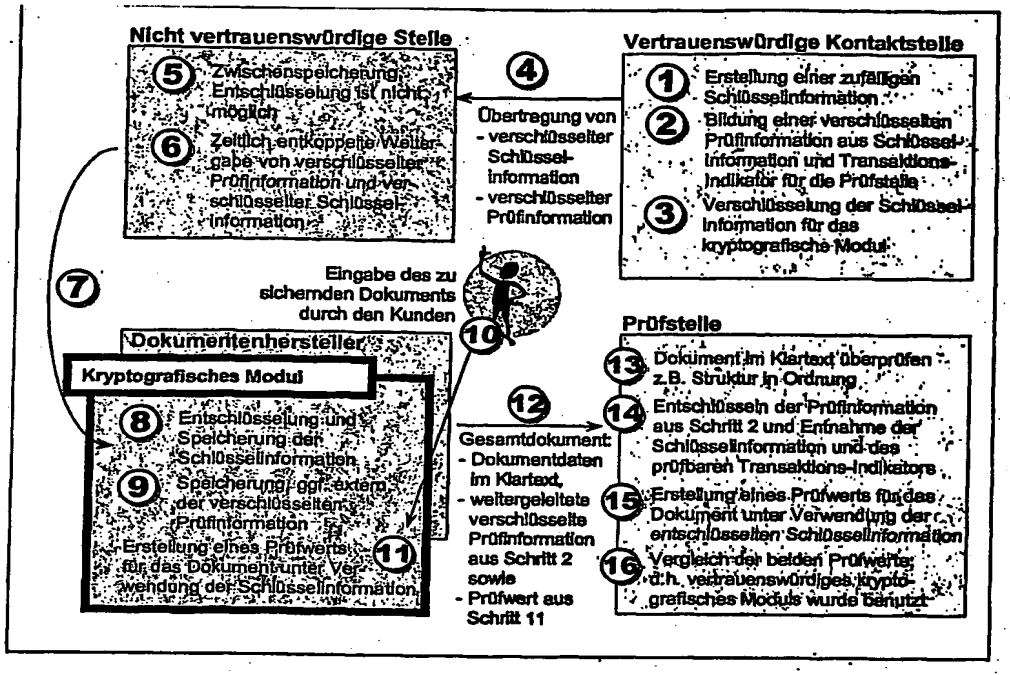

FIG. 3